COMMITTEE ACTION RESOLUTION #1

I OBJECTIVE

A) To take technical positions on policies, regulations guidelines and other issuances that bear on the computer security position of the Intelligence Community

B) This objective is intended to be responsive to DCID NO. 1/11, (attachment 2), paragraph 1 and 6.

II PROPOSED ACTION ITEMS

These action items are proposed by CAR 1, in order to meet the objectives during the coming year:

A) A Review for changes required in community policies, standards and procedures as opposed to changes that can be made at the individual agency level.

B) Clarification of terminology and definitions in DCID 1/16 to insure uniform application of policy by community members.

C) Define the security standards and individual agency security responsibility for the networking of computers among community member organizations.

D) Define individual agency security responsibility and authority over a contractor organization which is simultaneously processing and/or storing classified data for two or more Intelligence Community Agencies.

E) Determine responsibility for authorization and access to a classified DP system resident in one Intelligence Agency but accessed via remote terminals by other Intelligence Agencies.

cars: 11-16-78
h.c.faust

Comments on Committee Action Resolutions:

CAR # 2: a. Formulate and Recommend to DCI Resource Programming Objectives for Computer Security and

b. Foster and Monitor Agressive Program of R&D to Resolve Technical Problems associated with Protection of Computer Operations.

(1) To assure effective and efficient use of resources

(2) To avoid duplication of efforts

(3) To counter current and foreseen vulnerabilities and threats

(4) To assure effective resolution of technical problems

1. Scope the Task

a. Define the customer base (i.e., users/data/systems/networks) for which the Computer Security Subcommittee has responsibility.

b. Determine the needs -- based on known and predicted threats and vulnerabilities and operational requirements.

1) Receive inputs from CAR #3 (i.e., objectives (1), (2),(3))

2) Receive inputs from R&D Subcommittee's Computer Security Working Group

3) Request Statement of Requirements from customer base.

4) Review Policy technical requirements.

5) Review Systems Develoment Plans

6) etc.

c. Identify existing R & D projects

1) Update last year's session of presentations to Subcommittee

2) Review R & D Plans (I.C. Members, Mildeps, etc.)

3) Prepare inventory of R&D projects

a) Intelligence Community sponsored

b) Other Government sponsored

c) Industry R & D

d. Relate existing R & D Projects to Needs

1) Identify overlaps and resource utilization not supported by a validated or anticipated requirement

2) Identify voids, requirements not being addressed

2. Formulate a Five Year R & D Plan

a. Use above information as a baseline

b. Establish priorities

3. Develop a Management Mechanism for Executing the Plan

a. Obtain community-wide endorsement of the Plan, including priorities

b. Recommend to DCI the continuation and additional support for existing R & D projects that respond to the Plan

c. Identify agencies that could best sponsor new R & D projects required by the Plan

1) Recommend DCI task these agencies

d. Identify centers of interest (OPIs) for each major area of R & D

e. Establish a mechanism for technical information exchange and dissemination of research studies, development plans and products.

1) Periodic workshops or seminars

2) Through the training program (CAR #4)

3) Through a central information repository (CAR #3)

4) Participation in DoD Computer Security Consortium

5) Publications (including policy)

f. Periodically assess the R & D Plan and realign projects based on current technical developments, problems and requirements

4) How is this going to get done?

1) manning

2) dollars

.bp 3) When first plan ready (draft)?

CAR #4: Develop Coordinated Program of Computer Security Training and Indoctrination for Intelligence Community.

1. Scope the Task

a. Define "student bodies" for which the Computer Security Subcommittee has "training" responsibilities.

1) I. C. Staff Members -- SECOM, R&D Subcommittee (Tech Surveillence Teams), etc.

2) I. C. Agencies -- Executive Managers, Computer Security Personnel, ADP Managers, etc.

3) Etc.

b. Identify learning needs of student bodies.

1) Management/Executive Level

2) Policy/Decision-makers

3) Implementers

4) Users

5) Etc.

c. Define responsibility/role of Subcommittee

2. Outline subject matter for various student audiences

3. Determine how best subject matter can be delivered to student bodies.

a. Existing programs

b. New programs

c. Total courses, lectures, workshops, etc.

4. Establish training policy

a. Who should have what training by when

b. Monitoring of training program

c. Recognition of training undertaken (certificate, accreditation, etc.)

5. Execute Training program

a. Locations (Staff College, NCSchool, DODCI, etc.)

b. Staff

c. Course Development

d. Advertisement, Registration

e. Contracts (external, internal government)